UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte HEZI FRIEDMAN, GADI ELICH, OHAD FALIK,
and DAVID BRIEF

Appeal 2007-1418
Application 09/862,986
Technology Center 2100

Decided: August 7, 2007

Before HOWARD B. BLANKENSHIP, ROBERT E. NAPPI,
and St. JOHN COURTENAY III, *Administrative Patent Judges.*

NAPPI, *Administrative Patent Judge.*

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 6(b) of the Final Rejection of claims 2, 8 through 10, 13, 15, 18 through 20. The Examiner has indicated that claims 3 through 7, 11, 12, 14, 16, and 17 contain allowable subject matter, and claim 1 has been canceled. For the reasons stated *infra,* we will not sustain the Examiner's rejection of these claims.

INVENTION

The invention is directed to an apparatus that provides a secure Universal Serial Bus (USB) link between peripheral devices and a host machine. See page 12 of Appellants' Specification. Claim 2 is representative of the invention and is reproduced below:

> 2. An apparatus for providing a secure serial bus (USB) comprising a secure channel for transferring data, wherein said apparatus comprises a secure USB domain device coupled to an external host computer, wherein said secure USB domain device comprises elements that are not accessible by said external host computer.

REFERENCE

The reference relied upon by the Examiner is:

Flannery	U.S. 5,799,196	Aug. 25, 1998
Rawlins	U.S. 6,216,183 B1	Apr. 10, 2001
Ben-Dor	U.S. 2002/0141418 A1	Oct. 3, 2002 (filed Mar. 19, 1999)
Lemay	U.S. 2002/0144115 A1	Oct. 3, 2002 (filed Mar. 30, 2001)

EXAMINER'S REJECTIONS

Claim 2 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Rawlins.

Claims 8 through 10, 13, and 15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Flannery and Rawlins.

Claim 18 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Flannery, Rawlins, and Lemay.

Claim 20[1] stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Flannery and Rawlins, and Ben-Dor.

ISSUES

Appellants contend that the Examiner's rejection of independent claim 2 is in error. Appellants assert that Rawlins does not teach the claim 2 limitation "wherein said secure USB domain device comprises elements that are not accessible by said external host computer." Br. 6-7. Specifically, Appellants argue that Rawlins teaches two modes of operation and that "[t]he fact that accessibility is allowed during secure operations does not imply that there is no accessibility during normal operations." Br. 7, Reply Br. 4.

In response, the Examiner states, on page 9 of the Answer:

> The problem with the appellant's [sic] arguments is that it is based on the wrong analogy, that the memory is within USB host controller 30. However the controller only transfer [sic] the target address of the USB device to the memory system 18 location. Therefore only authorized user that have [sic] access to the location of the memory may use the address of the target USB device in order to access it. Therefore the limitation "wherein said USB domain device comprises elements that are not accessible by said external host computer" is

---

[1] The Examiner's statement of rejection on page 6 of the Answer identifies claims 8-10, 13, and 15 as rejected based upon Flannery, Rawlins, and Ben-Dor. However, the analysis supporting the rejection only addresses claim 20. Thus, we consider the statement of the rejection to contain a typographical error and that only claim 20 is rejected over Flannery, Rawlins, and Ben-Dor. This is consistent with Appellants' Briefs and the Examiner's response to Appellants' arguments.

> met since the domain is secure by providing only authorized access and not accessible otherwise.

Thus, Appellants' contentions present us with a first issue, whether Rawlins teaches or suggests the claim 2 limitation of "said secure USB domain device comprises elements that are not accessible by said external host computer."

Appellants argue that the Examiner's rejection of claim 8 is in error as the combination of Flannery and Rawlins does not teach a secure USB domain device capable of blocking outgoing data flow, forwarding outgoing data flows of encrypted information or forwarding outgoing data flows of non-confidential information. Br. 8. On page 7 of the Reply Brief, Appellants assert that claim 8 recites that the USB domain device, not the host computer, perform the blocking and forwarding.

In response, the Examiner states, on page 10 of the Answer:

> The limitation "blocking outgoing data flows of confidential information" is met by the fact that in secure mode the access to the USB device and the flow from USB device is block [sic] unless authorized. The limitation of forwarding outgoing data flows of encrypted confidential information and forwarding outgoing data flows on non-confidential information" is met by the fact that once the authorized access to a USB device by access to the address in memory 18 is given[,] the flow of data (confidential or non confidential, encrypted or non-encrypted) is granted in either direction.

Thus, Appellants' contentions present us with a second issue, whether the combination of Flannery and Rawlins teaches or suggests a USB domain

device which performs one of the claimed functions of blocking or forwarding.

FINDINGS OF FACT

Rawlins teaches a system to secure information input thorough a USB device. Abstract. The system uses a "southbridge," item 26 which is connected to the host computer's PCI bus and contains a USB host controller and a USB bus. Col. 6, ll.4-16. Thus, the southbridge is part of the host computer. The bridge contains a USB controller, which includes; a data buffer, target endpoint address registers and System Management Interrupt (SMI) registers. Fig 2, l. 66- col. 7, l. 10. A target endpoint address is the address of a USB device. See col. 2, ll. 66-67. The target endpoint address register contains the address of USB devices to have secured data transfer to the host. The USB controller monitors the target endpoint address of information on the USB bus and compares it to the addresses in the target endpoint address register. If there is a match, the USB controller will initiate a SMI signal. Col. 3, ll. 5-10. Thus, the SMI signal initiates a secure transfer of information from the USB device associated with the target endpoint address and a specific secure memory location in the host computer. Col 3. ll. 10-15. This secure memory address is not normally accessed and is not known to a user who does not know the target endpoint address. Col. 3, ll. 15-20. It is by keeping these addresses secret that the USB device provides protection against unwarranted intrusions. Col. 3, ll. 20-25.

Flannery teaches a method whereby a self powered USB device can power a host computer's continually powered logic while the computer's power is off. Abstract. Flannery teaches that host computers have a USB. Col. 2, ll 12-15.

ANALYSIS

First issue:

Claim 2 recites, "wherein said secure USB domain device comprises elements that are not accessible by said external host computer." The Examiner's rejection relies upon Rawlins' disclosure in column 3, lines 7 through 26, to teach this limitation. See Answer p. 4 and 9. The Examiner states that "only authorized user[s] that have access to the location of the memory may use the address of the target USB device in order to access it."

We agree with the Examiner's finding that Rawlins teaches that only authorized users have access to the address of the target USB device. See findings of fact *supra*. However, we disagree with the Examiner's finding that Rawlins teaches the USB controller comprises elements not accessible by the host computer. We find the USB controller, by being on the southbridge connected to the PCI bus, is part of the host computer. Also, Rawlins does not discuss that address locations, of either the secure main memory or the USB device (target endpoint address), are inaccessible by the host computer. Rather, Rawlins relies upon the addresses being unknown to users, as the method of providing secure transfer of data. Further, we find no convincing evidence of record to show that modifying Rawlins such that the USB controller would comprise elements not accessible by the host

computer is a predictable variation of Rawlins. Accordingly, we reverse the Examiner's rejection of claim 2.

Second issue:

Independent claim 8 recites "at least one host computer capable of supporting USB input/output devices, said computer comprising a USB bus ... a secure USB domain device capable of at least one of: blocking outgoing data flows..." Thus, as Appellants assert, on page 7 of the Reply Brief, independent claim 8 recites a USB domain device separate from the host computer which performs one of the recited functions of blocking and forwarding. Independent claim 15 recites similar limitations. The Examiner's rejection of independent claims 8 and 15 relies upon Rawlins' teaching of the USB controller as a USB device capable of blocking and forwarding. Answer 5. However, as discussed *supra* in our findings of fact, the USB controller (an element of the southbridge) is part of the host computer and provides the host computer's USB bus. We do not find that Rawlins teaches a USB device separate from the computer which performs the claimed functions of blocking and forwarding. As discussed in our findings of fact, Flannery teaches a computer system with a USB bus. However, Flannery does not teach a USB device separate from the computer which performs the functions of blocking and forwarding, as claimed. Thus, we find no convincing evidence of record to show that modifying Flannery and Rawlins to include a USB device separate from the computer which performs the claimed functions of blocking and forwarding is a predictable use of prior art elements. Accordingly, we reverse the

Examiner's rejection of independent claims 8, 15 and the dependent claims 9, 10 and 13.

Claim 18 depends upon claim 15 and is rejected over Flannery, Rawlings, and Lemay. Claim 20 depends upon claim 15 and is rejected over Flannery, Rawlings, and Ben-Dor. The Examiner did not find, nor are we able to find, that either Lemay or Ben-Dor teaches or suggests a USB device separate from the computer which performs the functions of blocking and forwarding as recited in independent claim 15. Accordingly, we reverse the Examiner's rejection of claims 18 and 20 for the reasons given with respect to claim 15.

CONCLUSION

We consider the Examiner's rejection of claim 2 to be in error as we do not find that Rawlins teaches or suggests the limitation of "said secure USB domain device comprises elements that not accessible by said external host computer" (Claim 2).

We consider the Examiner's rejection of claims 8 through 10, 13, 15, 18 through 20 to be in error as we do not find that the combination of Flannery and Rawlins teaches or suggests a USB domain device which performs one of the claimed functions of blocking or forwarding.

ORDER

For the forgoing reasons, we will not sustain the Examiner's rejections under 35 U.S.C. § 103. The decision of the Examiner is reversed.

REVERSED

pgc

William A. Munck
Novakov Davis & Munck, P.C.
13155 Noel Road, Suite 900
Dallas TX 75240